Advanced Slide Attacks Revisited: Realigning Slide on DES

Raphael C.-W. Phan

Information Security Research (iSECURES) Lab,
Swinburne University of Technology (Sarawak Campus),
93576 Kuching, Sarawak, Malaysia
rphan@swinburne.edu.my

Abstract. Slide attacks are powerful tools that enable the cryptanalyst to break ciphers with up to 4-round self-similarity. This paper introduces an advanced sliding technique that breaks ciphers with self-similarity more than 4 rounds, and even allows for sliding encryptions with dissimilar rounds in the middle of the slide. In particular, we present the *realigning slide attack* on variants of 14-, 15- and full 16-round DES. We hope our results will spur more effort into ways to extend the slide attacks to apply to larger classes of block ciphers with complex key schedules.

1 Introduction

The *slide attack* was introduced by Biryukov and Wagner in 1999 as a means to attack block ciphers by exploiting slight weaknesses in their key schedules [5]. A year later, the same authors presented advanced slide attacks [6], namely the *complementation slide* and *sliding with a twist* that could attack ciphers with slightly more complex key schedules. Now that 5 years have passed since then, it is natural to wonder if there are other ways to extend these slide attacks.

The DES' linear key schedule surprisingly resists all previously known slide and related-key [2,11,12] attacks, thus it is of major interest to show how it can be susceptible to slide attacks. Note however that linearity itself does not automatically imply weakness against such attacks. However, linear key schedules mean that relationships between round keys are much simpler both to exploit and possibly control, thus may have a higher chance of causing self-similarities. But DES has so far proven this wrong.

We introduce an advanced slide attack, the *realigning slide attack* by using a novel sliding technique that allows for sliding encryptions with dissimilar rounds in middle of the slide. Previously known sliding techniques would fail under this circumstance. We illustrate this new approach on DES variants, including the full 16 rounds with the original key schedule for a fraction of all keys, and slightly tweaked key schedules for almost all keys. Although our attack on full DES has a higher complexity than the best known attack, i.e. standard linear cryptanalysis [17] and is more of theoretical interest, our results indicate the irregular structure of the DES key schedule still has some exploitable degree of self-similarity that is susceptible to more subtle forms of slide attacks.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 263–276, 2005.

This paper is organized as follows: In Section 2, we briefly describe conventional and previous advanced slide attacks. We develop an advanced sliding technique in Section 3, the realigning slide which is demonstrated on DES variants. We discuss some related work in Section 4. We conclude in Section 5 and outline some interesting open problems in relation to extending the slide attacks.

2 The Slide Attacks

The basic slide attack [5] considers ciphers where each round is identical to the other. The cryptanalyst is interested to find a plaintext pair, P, P' with corresponding ciphertexts, C, C' such that he gets two *slid equations* of the form:

$$P' = F(P) \tag{1}$$

$$C' = F(C), \tag{2}$$

where $F(\cdot)$ is the round function. To do so, he obtains a pool of $2^{n/2}$ known plaintexts (KPs) and corresponding ciphertexts (n is the block size), and uses this to form 2^n pairs. He then either directly checks if each pair satisfies the slid equations or has to make guesses of the keys in F while doing the checking. By the birthday paradox, he expects one slid pair satisfying the equations, upon which the key used in the F is recovered.

The limitation of this conventional technique is that it applies only to a small class of ciphers, particularly those whose key schedules cause identical round keys for each round, thus making each round identical to the other. This technique is basically a clever adaptation of the rotating subkey related-key attack[1] [2] to the non-related-key context, i.e. the requirement for related keys that cause identical or self-similar (repeating) round keys is eliminated by using ciphers with weak key schedules that themselves cause identical or self-similar round keys.

2.1 Advanced Sliding Techniques

The basic slide attack works on one-round self-similar ciphers, i.e. all round keys are identical, but when the self-similarity consists of more complex rounds, then further advanced sliding techniques have to be used. Two such techniques: complementation slide and twisting slide, were presented in [6].

The *complementation slide* applies particularly well to Feistel-like ciphers and amplifies their two-round self-similarity into one-round self-similarity. The basic concept is to slide two encryptions such that the slid rounds, rather than being exactly identical to each other, have a constant difference due to dissimilar round keys that propagates with probability one from one end of the slid rounds to the other. In this way, the plaintexts and ciphertexts forming a slid pair are still related by one unslid round and the slid equations are similar to (1) and (2). The restriction is that the round keys must be inserted via the same

[1] In modern day terms, this is more suitably known as related-key slide attack.